

LINUCA - Asociación de Usuarios GNU/Linux en Cantabria

SNORT+MYSQL+ACID: Sistema de detección de intrusos open source.

Por Bolo (http://linuca.org/todos.phtml?id_autor=1) creado el << 10/08/2002 16:35 >> y modificado por última vez el << 10/08/2002 16:35 >>

En esta ocasión, los avispados linucadictos conoceremos paso a paso la instalación y configuración de snort, un sistema open source de detección de intrusos. Configuraremos snort en debian, para que loguee sobre MySQL y así poder usar ACID (aplicacion web) para el analisis de los logs. Snort se autoactualizará y nos enviara informes diarios al buzon de correo.

Para empezar trataremos las diferentes clases de detectores de intrusos que existen y definiremos esas siglas tan raras que se han puesto ahora tan de moda (IDS, NIDS, HIDS, etc) :

1- IDS, Intrusion Detection System , a veces llamado HIDS, H de Host

Los IDS, en principio, solo capturan alertas ocurridas en el host local donde estan instalados. Aunque, por extension, todos los Sistemas de Intrusion, del tipo que sean, son tambien llamados IDS.

2- NIDS - Network Intrusion Detection System

Estos sistemas detectan alertas snifando el trafico que pasa por su tarjeta de red. Por lo que si son colocados en los lugares correctos (p.e. los firewalls, gateways etc) nos detectan los ataques producidos a cualquiera de los hosts de nuestra red. Los DIDS (Distributed Intrusion Detection System) son NIDS donde los sensores que detectan y recolectan información estan distribuidos en diferentes puntos/hosts en la red. Snort, como no, tambien puede actuar como NIDS.

- **SNORT**

Snort es, basicamente, un sniffer que rastrea los paquetes que circulan por la red en busca de patrones de ataque, escaneos de puertos y demás actividad sospechosa. Cuando un paquete casa con algún patrón establecido en las reglas de configuración, se logea. Así sabremos cuando, de donde y como se produjo el ataque.

- **INSTALACIÓN DE SNORT+MYSQL+ACID.**

Nuestro objetivo va a ser configurar snort para que logee en la base de datos MySQL, para despues instalar ACID, una aplicación web escrita en PHP que nos permitirá acceder a toda la información que proporciona snort de manera ordenada y sencilla. ACID nos permitirá realizar búsquedas de todo tipo en la base de datos, estas búsquedas pueden ser por ip fuente/destino, por fecha, por ataque, por protocolo, realizar informes, graficas, etc, una autentica gozada.

Ademas de esta herramienta, que nos va a facilitar enormemente el analisis de los logs..., a mi personalmente

me gusta que tambien me envie por mail informes diarios de la actividad registrada, para no tener que conectarme al web cada día y mirar que hay de nuevo. Para conseguir esto, habilitaremos, ademas del logueo a MySQL, el logue sobre ficheros ordinarios ya que la mayoria de las herrmientas de reporte automático que hay para snort no soportan el acceso a bases de datos.

Bueno, ahora que sabemos un poco de que va esto, pasamos a la parte práctica:

Para la primera etapa de la instalación, necesitaremos apt-getar esto:

```
apt-get install mysql-server
apt-get install snort-mysql
```

Vale, bien, ya tenemos instalado la base de datos MySQL y snort con soporte para la misma. Ahora, configuraremos MySQL creando la base de datos de snort, con las tablas necesarias y para finalizar crearemos el usuario para que Snort puede acceder.
Fijar password de root de MySQL (si es una instalación limpia y no lo has echo aún) :

```
$mysqladmin -uroot password nueva-pass
```

Creamos la nueva base de datos :

```
$mysqladmin -uroot -p create snort
```

Existe en el paquete snort-mysql un archivo con el volcado de tablas que necesita Snort para loguear :

```
$gunzip /usr/share/doc/snort-mysql/contrib/create_mysql.gz
$mysql -uroot -p snort < /usr/share/doc/snort-mysql/contrib/create_mysql
```

Ya tenemos las tablas listas, ahora creamos el usuario para snort :

```
$mysql -uroot -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 20 to server version: 3.23.51-log

Type ’help;’ or ’\h’ for help. Type ’\c’ to clear the buffer.

mysql>grant all on snort.* to snort@localhost identified by ’xxxxxx’;
Query OK, 0 rows affected (0.13 sec)
mysql> flush privileges;
Query OK, 0 rows affected (0.19 sec)
```

Ahora vamos a por Snort...

Las firmas de ataques que usa snort para generar alertas se encuentra en el directorio /etc/snort. Estas firmas se encuentran en los arichivos con extension *.rule y el nombre del archivo hace referencia al tipo de alertas que contienen (netbios.rules, exploit.rules, x11.rules, etc).

El siguiente paso es configurar snort editando su fichero de **configuración /etc/snort/snort.conf**. El fichero se divide en 4 partes fundamentales :

1- Configurarción de las variables de red para nuestro entorno.

En esta seccion asignaremos valores a las variables tales como la red que monitorizará snort en busca de ataques (HOME_NET), los servidores DNS (DNS_SERVERS), servidores smtp (SMTP_SERVERS), etc. Se recomienda establecer al menos los servidores DNS que utilizan nuestros equipos (sobre todo si teneis una red casera y tirais de dns externos) para evitar falsos positivos de portscanning.

2- Configurar los preprocesadores.

A partir de la versión 1.5 aparecieron los preprocesadores que permiten que las funcionalidades de snort sean extendidas por los usuarios proporcionando un sistema de acceso a los paquetes antes de que sean procesados por el motor de deteccion de snort.Para empezar, podemos dejar los valores por defecto que vienen. Si necesitais mas información, en el manual de usuario teneis todos los preprocesadores que vienen con el

paquete explicados muy sencilla y resumidamente.

3- Configurar los plugins de salida.

Los plugings de salidad nos permiten elegir de entre un gran variedad de formatos de salida. En el snort.conf vienen todas comentadas y con ejemplos. Nosotros vamos a configurar dos salidas (al fichero /var/log/snort/alert y a MySQL) simultaneamente. Añadiremos estas lineas :

```
#esto nos vuelca las alertas al archivo /var/log/snort/alert

output alert_full : alert

#esto configura el logeo sobre MySQL

output database: log, mysql, user=snort password=xxxxx dbname=snort host=localhost
```

4- Personalizar las reglas.

Este es el ultimo paso... si queremos deshabilitar algun grupo de reglas solo tenemos que comentar el include correspondiente. Por ejemplo :

```
#==========================================
# Include all relevant rulesets here
#
# shellcode, policy, info, backdoor, and virus rulesets are
# disabled by default. These require tuning and maintance.
# Please read the included specific file for more information.
#==========================================

include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-coldfusion.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/sql.rules
include $RULE_PATH/x11.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/netbios.rules
# include $RULE_PATH/backdoor.rules
# include $RULE_PATH/shellcode.rules
# include $RULE_PATH/policy.rules
# include $RULE_PATH/porn.rules
# include $RULE_PATH/info.rules
# include $RULE_PATH/icmp-info.rules
# include $RULE_PATH/virus.rules
```

Aqui vemos como se han comentado unos cuantos grupos como info, policy-info, backdoors, etc...

¡BIEN!, ya tenemos snort configurado y listo para rular... Le metemos un /etc/init.d/snort restart sin ningun tipo de miedo, y con ps aux | grep snort, miramos a ver si está arriba... Si hubiera problemas probad a arrancar snort desde la consola con "snort -c /etc/snort/snort.conf" para ver los errores.

El siguiente paso es meterle cera al ACID (Anlisys Console form Intrusion Databases). Esta herramienta entra dentro del proyecto AirCert, sponsorizado por el CERT. Este proyecto desarrolla herramientas de seguridad open source, con el ánimo de disponer de un entorno de detección de intrusios eficiente y de bajo coste.

Instalar **ACID** es tan facil como esto:

```
#apt-get install acidlab
#chown -R www-data:www-data /etc/acidlab
#vi /etc/acidlab/acid_conf.php
```

Aqui relleneramos los campo relativos a la base de datos...:

```
/* Alert DB connection parameters
```

```
* - $alert_dbname : MySQL database name of Snort alert DB
* - $alert_host : host on which the DB is stored
* - $alert_port : port on which to access the DB
* - $alert_user : login to the database with this user
* - $alert_password : password of the DB user
*
* This information can be gleaned from the Snort database
* output plugin configuration.
*/
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "xxxxx";
$alert_user = "snort";
$alert_password = "";

/* Archive DB connection parameters */
$archive_dbname = "snort_archive";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "snort_archive";
$archive_password = "zzzzz";
```

Existen dos usuarios que hay que rellenar, los del usuario con acceso a la bd snort, y los del de acceso a la snort_archive. Esta segunda base de datos será creada por acid para que el usuario pueda archivar alertas importantes.

Para crear esta segunda base de datos, hacemos tres cuartos de lo mismo de lo que hicimos para crear la base de datos de snort y el usuario :

```
# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 22 to server version: 3.23.51-log

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> grant all on snort_archive.* to snort_archive@localhost identified by 'zzzzz';
Query OK, 0 rows affected (0.05 sec)
mysql> flush privileges;
Query OK, 0 rows affected (0.19 sec)

mysql>
```

Ya está, para comprobar que todo a ido bien lanzamos el navegador y vamos a http://localhost/acidlab/. La primera vez que accedeis acid os informará de que tiene que crear algunos indices extra en la base de datos de snort para poder funcionar, seguid las instrucciones y al finalizar nos mostrará la consola de analisis de logs de snort. Nada mas echarle un vistazo se puede ver la potencia de esta herramienta ya que podemos filtrar y realizar busquedas casi bajo cualquier criterio que se nos ocurra. Pues ya hemos terminado, podeis probar el chiringuito haciendoos un escaneo de puertos (desde otro equipo en la red , no desde localhost que ahi snort no escucha) o pasaros el nessus. Por ultimo decir que el correo del administrador que recibe las informes de alertas diarias se encuentra en la variable DEBIAN_SNORT_STATS_RCPT del archivo /etc/snort/snort.debian.conf.

```
DEBIAN_SNORT_STATS_RCPT="correo@tuyo.com"
```

Para que el snort actualize las firmas de ataques automagicamente yo uso oinkmaster. Los descargais y lo descomprimis en /etc/snort/oinkmaster.

Editamos /etc/crontab y añadimos esta linea para que la actualización se produzca cada dia a las 2:30 de la madrugada.

```
30 2 * * * cd /etc/snort/oinkmaster; ./oinkmaster.pl -o /etc/snort/ 2>&1 | logger -t oinkmaster
```

Bueno, para terminar os pongo un **resumen-receta** de los comandos que hemos seguido para poner esto a punto :

```
#apt-get install mysql-server
#apt-get install snort-mysql
$mysqladmin -uroot password nueva-pass
$mysqladmin -uroot -p create snort
```

```
$gunzip /usr/share/doc/snort-mysql/contrib/create_mysql.gz
$mysql -uroot -p snort < /usr/share/doc/snort-mysql/contrib/create_mysql
mysql>grant all on snort.* to snort@localhost identified by 'xxxxxx';
#vi /etc/snort/snort.conf <- rellanar al menos la variable DNS_SERVERS y añadir las entradas de los
output plugins de alert_full: y database:
#apt-get install acidlab
#chown -R www-data:www-data /etc/acidlab
#vi /etc/acidlab/acid_conf.php <- editar los valores realtivos a los usuarios de acceso a mysql
mysql> grant all on snort_archive.* to snort_archive@localhost identified by 'zzzzz';
#vi /etc/snort/snort.debian.conf <- rellenar la variable DEBIAN_SNORT_STATS_RCPT con el correo que
recibira los informes diarios
#wget ftp://ftp.it.su.se/pub/users/andreas/oinkmaster/oinkmaster-0.6.tar.gz
#tar xpvzf oinkmaster-0.6.tar.gz
#mv oinkmaster-0.6 /etc/snort/oinkmaster
#vi /etc/crontab <- añadimos la entrada para ejecutar oinkmaster cada noche
```

Ahh, se me olvidadba comentar que es muy necesario poner un .htaccess en el directorio donde este acid para asi limitar el acceso a este servicio y si en vez de usar apache, tiramos de apache-ssl mejor que mejor, no mola nada si despues de montar todo se nos conectan al acid y nos borran las alertas no? En este articulo de bulma teneis un minitutorial de como hacerlo.

Bueno, eso es to, eso es to, eso es todo amigos xD y no olviden unixizarse y opensourcizarse...

Saludos a todos.

Enlaces :

- Snort http://www.snort.org/
- ACID http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html
- Oinkmaster http://nitzer.dhs.org/oinkmaster/

E-mail del autor: cesar@eureka-sistemas.com
Podrás encontrar este artículo e información adicional en: http://linuca.org/body.phtml?nIdNoticia=13